IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	**CRIMINAL NO. 4:11-CR-0062**
	:	
v.	:	**(Chief Judge Conner)**
	:	
JEREMY T. BRASHEAR	:	
	:	
	:	

MEMORANDUM

Presently before the court is the government's motion to quash defendant Jeremy T. Brashear's ("Brashear") subpoena *duces tecum*. (Doc. 90). For the following reasons, the court will grant the motion.

I. Factual Background[1]

In 2010, Trooper Matt Powell of the Pennsylvania State Police in Indiana, Pennsylvania, conducted an investigation of peer-to-peer file sharing programs that may have contained child pornography. (Doc. 70 at 6). Peer-to-peer file sharing networks enable computer users to share digital files between different network users. (Supp. Hearing Ex. 4). Trooper Powell used a program called Roundup 1.4.1 ("RoundUp") to search files available for sharing in the Gnutella peer-to-peer file sharing network. (Doc. 70 at 8). RoundUp is a modified version of the file sharing software PHEX. (Id. at 26-27). RoundUp utilizes a database of "hash values" from

[1] The parties are well familiar with the factual background of this case, and the court will recite only those facts relevant to the disposition of the instant motion. To the extent that the court provides facts that were not previously discussed in its memorandum and order (Doc. 69) disposing of Brashear's motion (Doc. 51) to suppress, the facts are based on the testimony presented at the suppression hearing.

files known to contain child pornography. (Id. at 10). This database enables law enforcement to identify files with hash values that match the hash values of known child pornography. (Id. at 10). RoundUp only identifies computer files that are available for downloading from a folder shared with the Gnutella network. (Id. at 25, 27-28; Supp. Hearing Ex. 1007).

During the course of his investigation, Trooper Powell downloaded two videos from the IP address 174.60.89.228 that contained child pornography. (Doc. 70 at 11). In addition, Trooper Powell identified numerous files associated with child pornography emanating from this same IP address. (Id. at 8). Comcast Cable Communications ("Comcast") controlled the subject IP address. (Id. at 7). Trooper Powell alerted Corporal Thomas Trusal to his findings. (Id. at 6). Accordingly, Corporal Trusal obtained a subpoena ordering Comcast to provide subscriber and billing information for this IP address. (Id. at 14). Based upon an aggregate of investigative materials, including the identification of the registered account holder, Corporal Trusal secured a search warrant for 1651 Kaiser Avenue, South Williamsport, Pennsylvania, 17702. (Id.)

Brashear resided in a trailer on the property of the 1651 Kaiser Avenue residence. As a result of information obtained through the execution of the search warrant, Brashear was arrested. (Id. at 113). Law enforcement eventually secured an additional search warrant for Brashear's trailer and laptop. (Id.) This search revealed child pornography. (Id.)

On February 24, 2011, a grand jury indicted Brashear for distributing, receiving, and possessing material constituting or containing child pornography, in violation of 18 U.S.C. § 2252A(a). (Doc. 1). On July 26, 2012, Brashear filed a motion (Doc. 51) to suppress, which the court denied on October 12, 2012. (Doc. 69). On July 25, 2013, Brashear filed an *ex parte* motion (Doc. 81) for the issuance and service of a subpoena to compel the Pennsylvania State Police ("PSP") to provide the source code for RoundUp. Defense counsel explained that he already obtained the PHEX source code and sought access to the RoundUp source code to compare the two. (Doc. 81 ¶¶ 29-31).

The court granted the motion on July 26, 2013. (Doc. 82). On September 23, 2013, Brashear filed a motion (Doc. 88) to continue trial and jury selection. In support, he averred that, as of that date, the PSP had not produced the required source code.[2] On October 17, 2013, the government filed a motion to quash the subpoena. (Doc. 90). The government alleges that compliance would be unreasonable and oppressive under Federal Rule of Criminal Procedure 17(c)(2). (Id. at 2). The motion is fully briefed and ripe for disposition.

[2] The government alleges that the PSP do not possess the RoundUp source code. (Doc. 90 ¶ 4; Doc. 91-1 Ex. 1 ¶ 11). Brashear counters that the PSP possess both the source code and the program itself. (Doc. 93 at 1, Ex. 1). The court's determination that the source code is not relevant in this case negates any need for resolution of this dispute.

II. <u>Discussion</u>

Brashear alleges that his subpoena is necessary to determine whether the use of the RoundUp program violated Brashear's Fourth Amendment rights, the Federal Electronic Communications Privacy Act ("FECPA"), 18 U.S.C. § 1510 *et seq*, the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("PA Wiretap Act"), 18 Pa. C.S.A. § 5701 *et seq*, and the Gnutella network protocol.[3] The government asserts that Brashear is attempting to improperly use Rule 17 as a discovery vehicle, that the source code is subject to the law enforcement privilege, and that the information sought is irrelevant because the use of RoundUp did not violate Brashear's Fourth Amendment rights, the FECPA, the PA Wiretap Act, or the Gnutella network protocol.

The issuance of a subpoena is governed by Federal Rule of Criminal Procedure 17. To obtain a subpoena under Rule 17, the moving party must establish the following:

> (1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general "fishing expedition."

[3] In Brashear's motion for a continuance of jury selection and trial, he also stated that he needs the source code in order "to make an intelligent determination of whether it is necessary for the defense to seek the services of an expert in the computer field to assist the defense at the time of trial." (Doc. 88 ¶ 22). Such a desire does not comport with the purpose of a Rule 17 subpoena and the Court's decision in <u>Nixon</u>.

United States v. Nixon, 418 U.S. 683, 699-700 (1974). The court must reconsider the Nixon standard when disposing of a motion to quash. United States v. Beckford, 964 F. Supp. 1010, 1028 (E.D.Va. 1997).

The court finds that the source code for RoundUp is not relevant because its use did not violate Brashear's Fourth Amendment rights, the FECPA, and the PA Wiretap Act. Further, any violation of the Gnutella network protocol is irrelevant. Thus, the court will not address the application of the law enforcement privilege or whether Brashear otherwise improperly utilized Rule 17 in seeking a subpoena.

A. Fourth Amendment

The source code for the RoundUp program is not relevant because investigating the use of a peer-to-peer file sharing program does not violate the Fourth Amendment's protection against unreasonable searches. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV. A typical Fourth Amendment analysis begins with analyzing whether the defendant possesses a reasonable expectation of privacy in the object being searched. Katz v. United States, 389 U.S. 347 (1967); Kyllo v. United States, 533 U.S. 27, 27-28 (2001). Numerous cases have held that there is no reasonable expectation of privacy in files made available to the public through peer-to-peer file sharing programs. See, e.g., United States v. Stults, 575 F.3d 834, 842-43 (8th Cir. 2009); United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008); United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008).

Brashear wishes to compare the modified source code for RoundUp with the original PHEX source code, but there is no need. The RoundUp program only accesses files shared through the file sharing network. (Doc. 70 at 25-28; Supp. Hearing Ex. 1007). By sharing files with the network, Brashear essentially shared those files with the public. He had no reasonable expectation of privacy over the files shared with Gnutella and, therefore, the use of the RoundUp program could not have violated his Fourth Amendment rights.

Brashear responds that, pursuant to United States v. Jones, 132 S. Ct. 945 (2012), the use of the RoundUp program constituted a physical trespass of Brashear's "effect" – the computer – and was therefore an unreasonable search.[4] In Jones, the Court addressed whether the warrantless installation of a GPS tracking device to the defendant's motor vehicle violated his Fourth Amendment rights. 132 S. Ct. at 948. The Court concluded that the defendant's "Fourth Amendment rights do not rise or fall with the Katz formulation" concerning the defendant's reasonable expectation of privacy. Id. at 950. Instead, the Court found that the defendant's motor vehicle was an "effect" and the warrantless physical trespass of that "effect" to obtain information or evidence constituted an unreasonable search under the

[4] Brashear also cites Florida v. Jardines, 133 S.Ct. 1409 (2013), for the same argument. In that case, law enforcement officers took a drug-sniffing dog to the defendant's front porch, where the dog alerted to the presence of narcotics. 133 S.Ct. at 1413. The Court held that it was unnecessary to determine whether the officers violated the defendant's expectation of privacy under Katz because the officers physically trespassed upon the curtilage of the defendant's home. Id. at 1414. Hence, Jardines is not on point with the case *sub judice*.

Fourth Amendment. Id. at 948. However, the Court noted that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to [the] Katz analysis." Id. at 953 (emphasis in original).

Several courts have rejected the application of Jones to the investigation of file sharing programs. See Russell v. United States, Civ. A. No. 11-1104, 2013 WL 5651358 at *8 (E.D. Mo. Oct. 16, 2013); United States v. Nolan, Crim. A. No. 11-82, 2012 WL 1192183 at *10-11 (E.D. Mo. Mar. 6, 2012); United States v. Brooks, Crim. A. No. 12-166, 2012 WL 6562947 at *5 (E.D.N.Y. Dec. 17, 2012); State v. Lemasters, Crim. A. No. 2012-12-028, 2013 WL 3463219 at *3-5 (Ohio. App. July 8, 2013). The court concurs with the rationale of these decisions. The investigation of a file sharing program does not involve any physical trespass onto a constitutionally protected area. Trooper Powell did not physically enter Brashear's home or access his computer. Instead, Trooper Powell simply used a program that identified child pornography available on a public peer-to-peer file sharing program. This investigation involves "the transmission of electronic signals without trespass" and does not implicate Brashear's Fourth Amendment rights under Jones.

B. The FECPA and the PA Wiretap Act

Brashear also alleges that the subpoena is relevant to determining whether the warrantless use of RoundUp violated the FECPA and the PA Wiretap Act. Brashear provides no explanation for how these statutes potentially apply in the case *sub judice* and the court is unaware of any possible violation of these laws.

C. Gnutella Network Protocol

Finally, Brashear states that the use of RoundUp violates Section 4.4 of the Gnutella network protocol, which requires that users who are able to download files must also be able to share files with others. (Doc. 81 ¶ 15). Trooper Trusal testified that RoundUp is only able to download files from another computer and is not able to upload any files. (Doc. 70 at 26). It is unclear how obtaining the RoundUp source code would shed any further light on this alleged violation. Moreover, Brashear does not posit how this alleged violation is relevant in the case *sub judice*. Indeed, application of the exclusionary rule is typically reserved for violations of a constitutional dimension. See United States v. Lombera-Camorlinga, 206 F.3d 882, 886 (9th Cir. 2000) (collecting cases).

III. Conclusion

The source code for RoundUp is simply not relevant to determining any issue in the case. There is no indication that the use of RoundUp violated Brashear's rights under the Fourth Amendment, the FECPA, or the PA Wiretap Act. The potential violation of the Gnutella network protocol is irrelevant. For the above-stated reasons, the court will grant the government's motion to quash. An appropriate order follows.

/S/ CHRISTOPHER C. CONNER
Christopher C. Conner, Chief Judge
United States District Court
Middle District of Pennsylvania

Date: November 18, 2013